IN THE CLAIMS

1. (Previously Presented) A method of authenticating the identity of a user, the method comprising:

a. placing, in sequence, each of a plurality of parts of the user's body on a biometric contact sensor at a sensing position;

b. obtaining from the sensor a data set of biometric contact characteristics for each of the plurality of body parts;

c. comparing each data set with authentic versions stored in a database;

d. determining whether each of the plurality of parts of the user's body are placed on the biometric contact sensor at a sensing position within a predetermined period of time; and

e. issuing an authentication signal if the data sets satisfactorily match the corresponding authentic versions and the plurality of parts of the user's body are placed on the biometric sensor within the predetermined period of time.

2. (Original) A method according to claim 1, wherein the body parts are the user's fingertips and the biometric contact sensor is a fingerprint sensor.

3. (Cancelled)

4. (Original) A method according to claim 1, further comprising the step of confirming that the sequence of data sets was obtained in a predetermined order before issuing the authentication signal.

5. (Original) A method according to claim 1, wherein the data sets are compared with the authentic versions using a minutiae based algorithm.

6. (Original) A method according to claim 1, wherein the data sets are compared with the authentic versions using a correlation based algorithm.

7. (Previously Presented) Apparatus for authenticating a user, the apparatus comprising a fingerprint sensor operable to sensing only one fingerprint at a time, and a processor and a database adapted to perform a method according to claim 1.

8. (Original) Apparatus according to claim 7, wherein the fingerprint sensor is a capacitive sensor.

9. (Original) Apparatus according to claim 7, wherein the fingerprint sensor is an optical sensor.

10. (Original) Apparatus according to claim 7, wherein the fingerprint sensor is a thermal sensor.

11. (Original) Apparatus according to any of claim 7, further comprising a data input device.

12. (Original) Apparatus according to claim 11, wherein the data input device is a keypad.

13. (Original) Apparatus according to claim 11, wherein the data input device is a smart card reader.

14. (Previously Presented) A method of authenticating the identity of a user, the method comprising:

a. obtaining a sequence of data sets of biometric characteristics of the user, each data set relating to one of a plurality of parts of the user's body;

b. comparing each data set with authentic versions stored in a database;

c. monitoring the order in which the sequence of data sets was obtained;

d. determining whether the sequence of data sets is obtained within a predetermined period of time; and

e. issuing an authentication signal if the data sets satisfactorily match the corresponding authentic versions, the sequence of data sets was obtained in a predetermined order, and the sequence of data sets was obtained within the predetermined period of time.

15. (Original) A method according to claim 14, wherein at least one of the plurality of parts of the user's body is a fingertip.

16. (Original) A method according to claim 14, wherein at least one of the plurality of parts of the user's body is a retina.

17. (Original) A method according to any of claim 14, wherein at least one of the plurality of parts of the user's body is the user's face.